



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/824,930

04/15/2004

Thomas A. Gentles

1842.047US1

7285

70648

7590

11/28/2008

SCHWEGMAN, LUNDBERG & WOESSNER/WMS GAMING

P.O. BOX 2938

MINNEAPOLIS, MN 55402

EXAMINER

KIM, ANDREW

ART UNIT

PAPER NUMBER

3714

MAIL DATE

DELIVERY MODE

11/28/2008

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/824,930	<b>Applicant(s)</b> GENTLES ET AL.	
	<b>Examiner</b> ANDREW KIM	<b>Art Unit</b> 3714	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 07 August 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-18 and 20-30 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 and 20-30 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                       | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | Paper No(s)/Mail Date. _____                                      |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>8/7/08</u> .  | 6) <input type="checkbox"/> Other: _____                          |

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to the amendment filed on 8/7/08 in which:

- Response to claims rejection have been filed.
- Claim(s) 1-16, 20-30 are pending.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

**Claims 1-16, 21 and 23-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martinek et al. (US 7,043,641), “Martinek” in view of Ellison (US 6,073,237 A), “Ellison”.**

Claim 1. Martinek discloses a method performed by a gaming system server, the method comprising:

authenticating a gaming terminal's identity (col. 10:19-27); (It is inherent that a gaming terminal's identity is authenticated by code).

When the gaming terminal's identity is authenticated, then:

applying an encryption technique to encrypt a gaming software program, which produces an encrypted gaming software program (abstract, col. 6, 8:52-64); and

transmitting the encrypted gaming software program to the gaming terminal (abstract, col. 6).

Martinek substantially discloses the invention as claimed but fails to explicitly teach that the encryption technique is applied after authentication. Instead, Martinek discloses authentication of the gaming terminals and encryption in data in no set order. However, in an analogous reference, Ellison discloses first authenticating a terminal and then encrypting the data for transmission (3:43). By ordering the steps in this manner, the

server only uses valuable processing time encrypting data requested by authenticated receivers. This reduces pointless processing and encrypting of data requested by an unauthenticated receiver because the data would not be sent to the unauthenticated receiver anyway. In addition, it would hardly be advantageous to send sensitive information before authenticating the receiver. Therefore, one of ordinary skill in the art at the time of the invention would have found it obvious to first authenticate the gaming terminal before encrypting the data to save processing power and time as desirably taught by Ellison.

Claim 2. Martinek discloses receiving a request to download the gaming software program from the gaming terminal (col. 5:41).

Claims 3 ,4. Martinek discloses wherein authenticating the gaming terminal's identity comprises: receiving a gaming terminal digital certificate from the gaming terminal (col. 6:1-23); and authenticating the gaming terminal's identity based on the gaming terminal digital certificate (col. 6, 10).

Claim 5. Martinek discloses generating a session key to use in applying the encryption technique (col. 6:1-23, 12:25-39).

Claim 6. Martinek discloses wherein the encryption technique is selected from a group of encryption techniques that includes a symmetric encryption technique and an

asymmetric encryption technique (6:1-23, 10:19-39).

Claim 7. Martinek discloses wherein the symmetric encryption technique is an encryption technique that uses a one-time session key (6:1-23, 10:19-39, 12:25-39).

Claim 8. Martinek discloses wherein the asymmetric encryption technique is selected from a group of asymmetric encryption techniques that includes a public key encryption technique, and a multiple-key public key encryption technique (col. 6).

Claim 9. Martinek discloses

establishing a public-private key-pair, which includes a public key and a private key (col. 6); and generating the gaming terminal digital certificate, which includes a digital certificate that is signed with the private key (col. 10:13-39).

Claim 10. Martinek discloses a method performed by a gaming terminal, the method comprising:

authenticating a gaming system server (col. 6:38-50);

when the gaming server's identity is authenticated (10:62-11:8)

receiving an encrypted gaming software program from the gaming system server (col. 6:38-50); and

applying a decryption technique to decrypt the encrypted gaming software program, which produces a gaming software program (fig. 4).

Claim 11. Martinek discloses sending a request to download the gaming software program to the gaming system server (col. 5:41).

Claim 12. Martinek discloses wherein authenticating the gaming system server's identity comprises: receiving a gaming system server digital certificate from the gaming system server; and authenticating the gaming system server's identity based on the gaming system server digital certificate (col. 6:38-50).

Claim 13. Martinek discloses wherein the decryption technique is selected from a group of decryption techniques that includes a symmetric decryption technique and an asymmetric decryption technique (col. 6:38-50).

Claim 14. Martinek discloses wherein the symmetric decryption technique is a decryption technique that uses a one-time session key (fig. 4 along with the related description).

Claim 15. Martinek discloses wherein the asymmetric decryption technique is selected from a group of asymmetric decryption techniques that includes a public key decryption

technique, and a multiple-key public key decryption technique (col. 6).

Claim 16. Martinek discloses establishing a public-private key-pair, which includes a public key and a private key; and generating the gaming system server digital certificate, which includes a digital certificate that is signed with the private key (col. 6, 10).

Claims 21, 23-25. Martinek discloses a server of a gaming system generating a public-key private-key key pair; encrypting the public-key private-key key pair to produce an encrypted public-key private-key key pair; generating a certification authority digital certificate request, the certification authority digital certificate request including a public-key associated with the encrypted public-key private-key key pair; decrypting the public-key private-key key pair; and signing the certification authority digital certificate request using the private-key of the public-key private-key key pair to form the certification authority digital certificate (col. 6, 10, 11:36-48, 12:25-39).

Martinek substantially discloses the invention as claimed but fails to explicitly teach that the encryption technique is applied after authentication. Instead, Martinek discloses authentication of the gaming terminals and encryption in data in no set order. However, in an analogous reference, Ellison discloses first authenticating a terminal and then encrypting the data for transmission (3:43). By ordering the steps in this manner, the server only uses valuable processing time encrypting data requested by authenticated receivers. This reduces pointless processing and encrypting of data requested by an



unauthenticated receiver because the data would not be sent to the unauthenticated receiver anyway. In addition, it would hardly be advantageous to send sensitive information before authenticating the receiver. Therefore, one of ordinary skill in the art at the time of the invention would have found it obvious to first authenticate the gaming terminal before encrypting the data to save processing power and time as desirably taught by Ellison.

Claim 26. Martinek discloses further comprising authenticating the gaming terminal digital certificate (11:36-48).

Claim 27. Martinek discloses further comprising authenticating the gaming server digital certificate (col. 11).

Claim 28. Martinek substantially the invention as claimed but fails to explicitly teach whether the gaming terminal is authorized to access the gaming software program comprises checking an access control list. However, it is old and well known in the security art to maintain an access control list when one wishes to restrict which certain computers should or should not connect to another computer (e.g. wireless routers has had this feature for a while).

Claims 29 and 30. Martinek substantially discloses the invention as claimed but fails to explicitly teach determining that the gaming system a network address specified by a domain name. However, it is old and well known in the network security art to validate the network address specified by a domain name such that malicious users

cannot connect to the network unless the user has a network address specified by a domain name thereby eliminating most outsiders.

**Claims 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Martinek et al. (US 7,043,641), “Martinek” in view of Misra et al. (US 5,757,920), “Misra”.**

Claims 20, 22. Martinek discloses a method comprising: receiving a first signed digital certificate from a server, the first signed digital having an associated first public-key private-key key pair and having a first digital signature from an approval authority, the first digital signature formed by digitally signing the first public-key of the first public-key private-key key pair with a first approval authority private-key from a first approval authority public-key private-key key pair; authenticating the server based on the first signed digital certificate.

Martinek substantially discloses the invention as claimed but fails to explicitly teach double encryption as claimed. Instead, Martinek teaches single encryption (abstract, col. 6) and authentication from both a regulatory agency and a game code manufacturer. However, in an analogous reference, Misra discloses double encryption to insure the security, authenticity, and validity of the data being exchanged between the gaming terminal and the gaming server by transmitting randomly generated data by encrypting a one-way hash (5:56-6:16). Therefore, it would have been obvious to one or

ordinary skill in the art at the time of the instant invention to modify Martinek with double encryption to insure privacy, authentication and validity as taught by Misra.

### ***Response to Arguments***

Applicant's arguments filed 8/7/08 have been fully considered but they are not persuasive.

Applicant's arguments with respect to claims 1-18, 21, 23-25 have been considered but are moot in view of the new ground(s) of rejection.

Regarding claims 1, 10, 23, 24, 25, the Examiner respectfully asserts that identity of the terminal and the kernel, operating system etc. are one and the same. Without the operating system of a terminal it would not be any different from any other terminal. It is the code/kernel/operating system of a terminal which equates to the identity of the terminal and therefore when a terminal's operating system/kernel/code is verified so is the identity of the terminal. By the applicant's description of identity (paragraph 128 of the publication), it is clear that the identity pertains to the gaming software and data.

Regarding claims 20 and 22, refer to the Misra reference (5:56-6:16) in view of the new ground of rejection.

Regarding claim 21, locations have been interpreted as network addresses such as MAC addresses and the like.

### ***Conclusion***

Art Unit: 3714

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ANDREW KIM whose telephone number is (571)272-1691. The examiner can normally be reached on M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dmitry Suhol can be reached on 571-272-4430. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

11/27/2008 /A. K./

Examiner, Art Unit 3714

/Dmitry Suhol/  
Supervisory Patent Examiner, Art Unit 3714